PTOL-413A (10-07)
Approved for use through 10/31/2007 OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 10/797,773 First Named Applicant: Mark Ammar Rayes
Examiner: Shaifer Harriman, Dant B Art Unit: 2134 Status of Application: Non-Final Rejection

Tentative Participants:
(1) Karl Rees **(2)** _____
(3) _____ **(4)** _____

Proposed Date of Interview: June 30–July 3, July 9–11 **Proposed Time:** 11:00 AM– 3:00 PM **(AM/PM)**

Type of Interview Requested:
(1) [x] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [x] NO
If yes, provide brief description: _____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Rejection	14	Thomsen/Renda	[ ]	[ ]	[ ]
(2) Rejection	1	Thomsen/Renda	[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached

Brief Description of Arguments to be Presented:
Please see attached

An interview was conducted on the above-identified application on _____.
NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).
This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

/KarlTRees#58983/ _____
Applicant/Applicant's Representative Signature Examiner/SPE Signature

Karl Rees
Typed/Printed Name of Applicant or Representative

58923
Registration Number, if applicable

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

HICKMAN PALERMO TRUONG & BECKER LLP
San Jose, California

MEMORANDUM

DATE: June 26, 2008
TO: Examiner Shaifer Harriman; Tel. 571.272.7910; Fax. 571.27x.xxxx
FROM: Karl Rees; Tel. 408-414-1233; Fax 408-414-1076
SUBJECT: U.S. Patent Application No. 10/797,773 (Rayes, et al.)
Attorney Docket No. 50325-0865
3rd Office Action (Non-Final)

Proposed Agenda for Telephone Interview

I. Request clarification on rejection of Claim 14
   a. The Office Action does not clearly allege:
      i. What aspect of the references is a "malicious act"
      ii. What aspect of the references teaches "determining whether a malicious act caused the security event"
      iii. What aspect of the references teaches "if a malicious act caused the security event, then providing information . . . to a security decision controller."
      iv. What aspect of the references teaches "if a malicious act did not cause the security event, then removing the user from the elevated risk group."
II. Request clarification regarding suggestion / motivation to combine the references
III. Proposed Amendments to Claim 1
   a. Option 1: *see ¶¶ [0042]–[0043]*

1. (Previously presented) A method, comprising the computer-implemented steps of:
in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
determining a user identifier associated with the network device that has caused a security event in the network;
in response to the security event, causing the network device to acquire a ~~new~~ second network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
wherein causing the network device to acquire a new network address comprises causing the network device to request a new network address;
wherein the second subset of addresses is different from the first subset of addresses; and
configuring one or more security restrictions with respect to the new network address.

b. Option 2: *see ¶¶ [0003]–[0004]*

1. (Previously presented) A method, comprising the computer-implemented steps of:
in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
determining a user identifier associated with the network device that has caused a security event in the network;
wherein the security event is an event that indicates at least one of: a possible denial of service attack, possible IP address spoofing, extraneous requests for network addresses, and possible MAC address spoofing;
in response to the security event, causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
wherein the second subset of addresses is different from the first subset of addresses; and
configuring one or more security restrictions with respect to the new network address.